computing research

RESEARCH PAPER

Outsmarting the Smart: Entering the Age of Threat Hunting

October 2018

Sponsored by

Carbon Black.

CONTENTS

Executive Summary

Today's cyber criminals are constantly looking for new ways to attack. As soon as one threat is countered, another threat vector opens up. Attackers' aims are clear: They want to evade firms' prevention and detection controls and exploit vulnerabilities to gain access to networks, disrupt operations and target valuable data for theft or ransom.

Defending against these persistent and constantly evolving cyber- attacks can seem like a relentless game of 'whack-a-mole' for hard-pressed companies. Increasingly, the security professionals responsible for defending the network are realising that they need to understand the way adversaries think in order to stay ahead of emerging threats.

Adversaries are human too, and by thinking like the attacker and understanding their psychology and motivations, defenders can spot sophisticated attempts at secondary command and control and lateral movement that prevention systems alone would not pick up.

Rather than simply adding more technology and tools and responding when or after attacks occur, now is the time to take a more proactive approach to shift the balance of power away from attackers and back to defenders.

This is where threat hunting comes in. Threat hunting is the active pursuit and detection of the abnormal activity on the network that indicates potential compromise. Rather than a reactive activity carried out in response to a security alert, threat hunting is a continuous process that should become part of the security team's DNA. Threat hunters can make decisions quickly and wisely, using human judgement supported by machine intelligence to proactively defend against increasingly sophisticated cyber threat actors.

Given the right technology and support, threat hunters can continuously monitor entire infrastructures, closing the gap between IT and operations teams.

Indeed, building dedicated threat hunting capabilities into the security operations centre or similar business function offers multiple security benefits, as well as cost savings and demonstrable return on investment (ROI).

But how many firms are actually taking advantage of threat hunting today? *Computing* consulted more than 100 senior IT decision makers including IT directors, chief technology officers (CTOs) and chief information security officers (CISOs), across a variety of UK industries, working in organisations of between 50 and 5,000 employees.

The aim was to explore enterprises' current experience and readiness to embrace the significant potential of threat hunting. The survey also aimed to investigate the growing profile of cyber security threat insurance and assess its place inside the modern enterprise.

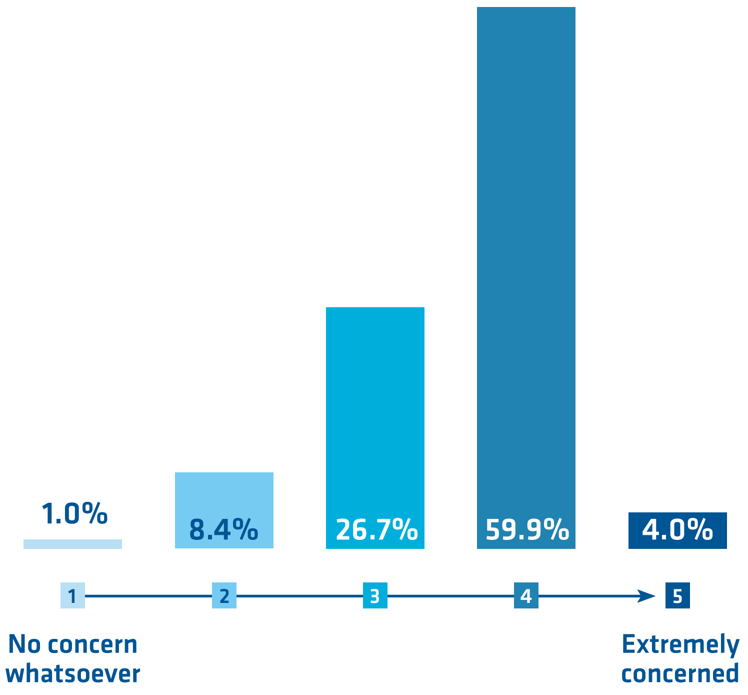
Assessing the threat landscape

To understand the benefits of threat hunting, it's important to consider the current state of security inside today's businesses. While cyber attacks are becoming more sophisticated, the network perimeter is eroding as firms move workloads into the cloud and employees become increasingly mobile.

Faced with this complex environment, many security teams are not able to keep pace with the swift evolution of techniques, tactics and procedures used by threat actors – who themselves are aiming to bypass existing prevention and detection control. All too often, security teams are limited to reactively dealing with attacks that happened in the past, instead of proactively getting on top of threats when they actually take place and anticipating future vulnerabilities and threat vectors.

This is despite the fact that organisations are concerned about how the enterprise threat landscape will evolve over the next six months. Nine out of 10 have medium to high levels of concern, according to the survey.

Fig. 1 : On a scale of 1 to 5 - 1 being "No concern whatsoever" and 5 being "Extremely concerned", what is your general level of concern about the enterprise threat landscape within the next six months?

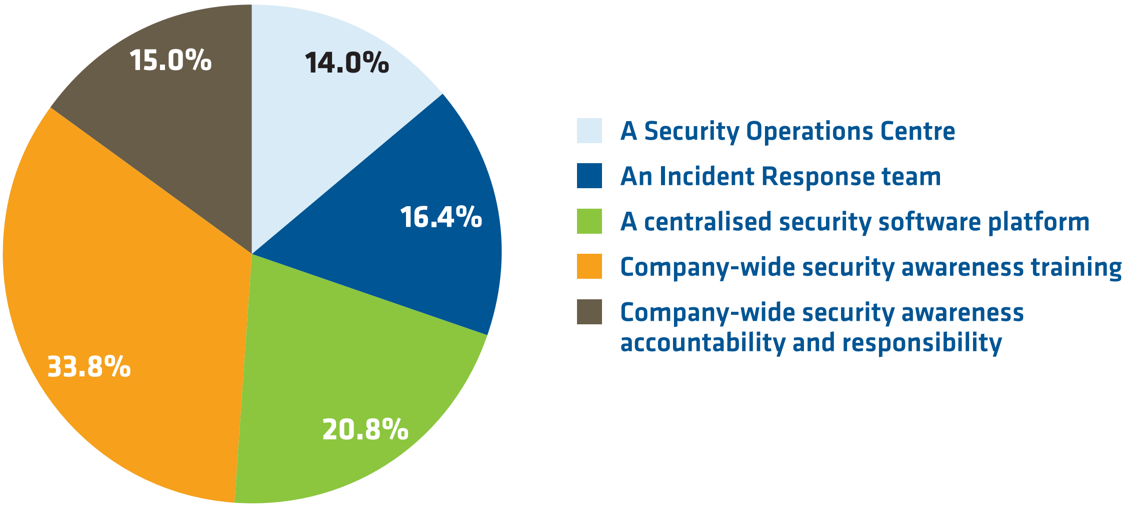


It is with this in mind that companies are utilising various security protocols, such as software platforms and employee training. The survey asked, **“Which of the following features does your enterprise security function utilise as a priority?”**

The survey found that the human element in security is increasingly important. Well over a third of firms (33 per cent) are employing company-wide security awareness training while an extra 15 per cent are also teaching accountability and responsibility. This helps users to consider the threats they face on a daily basis and their part in helping to counter attacks.

At the same time, one in five firms know technology can help support the people in their organisation: 21 per cent use a centralised security software platform. But despite increasing cyber threats, only a small number have a security operations centre (14 per cent) or incident response team (16 per cent).

Fig. 2 : Which of the following features does your enterprise security function utilise as a priority?

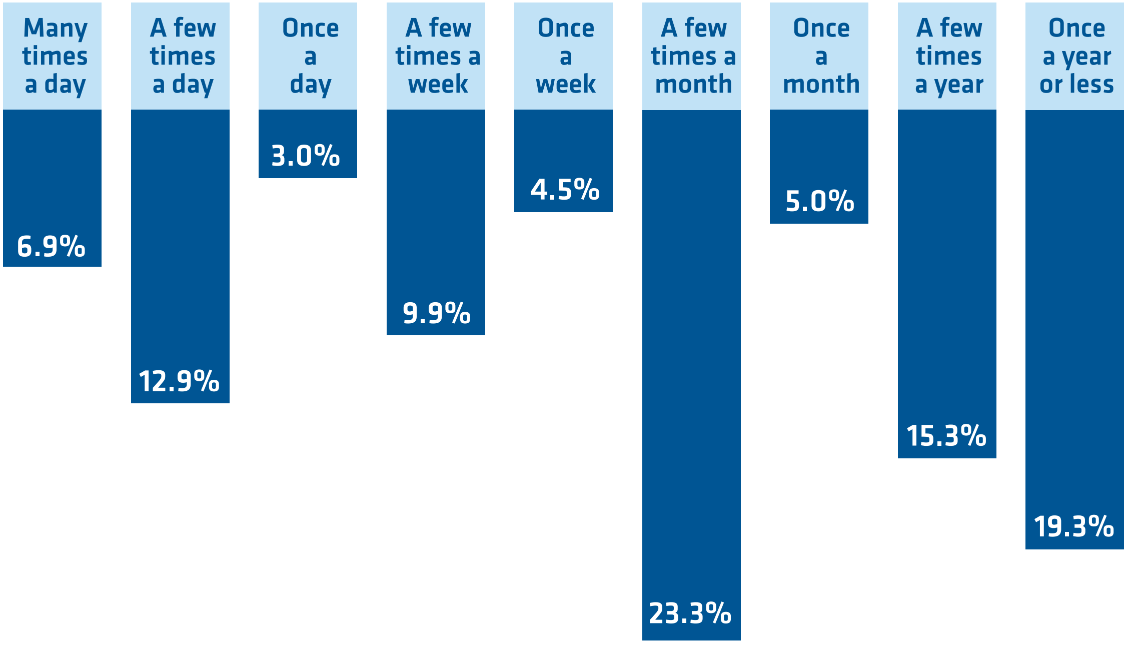


Outsmarting the smart: Harnessing the human element

Cyber criminals are human beings, so identifying, understanding and outsmarting them is key to gaining control of a firm’s security operations. We asked, **“How often does your security function encounter proven attacks by malicious actors (i.e. humans)?”**

The majority of respondents said they happen regularly, but one in five said they only encounter such attacks once a year or less. This is a concern because it could show that attacks are happening, but they are not necessarily being discovered. As attacks become increasingly sophisticated, cyber criminals aim to sidestep defences, gain an undetected foothold in a victim’s network and then live off the land, moving laterally within the organisation and maintaining persistence in preparation for launching attacks at will in the future. Detecting and rooting out these insidious attacks requires human intelligence to spot the anomalies that indicate malicious activity.

Fig. 3 : How often does your security function encounter proven attacks by malicious actors (i.e. humans)?



With the human element to security in mind, the survey also asked, **"To what extent does your organisation offer security training to its employees as standard practice?"**

Over half said, "We offer training to every single employee as standard". However, other firms offer training only to certain departments or levels of management (eight per cent and five per cent respectively). This is a concern at a time when all employees are vulnerable to falling for phishing emails and other emerging threats.

Proactive hunting

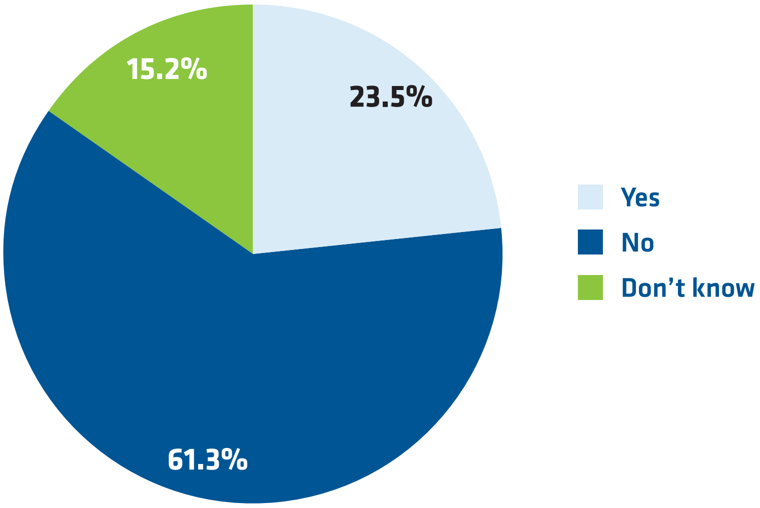
People talk about a "proactive" approach to security, but what exactly does this mean? Threat hunting is not simply watching and waiting for things to happen or investigating only in response to an alert.

Quite the opposite, in fact. The cyber security SANS Institute's definition of threat hunting is a focused and iterative approach to searching out, identifying and understanding adversaries entering a firm's networks. It goes beyond the technology used for defence: today's attackers can bypass monitoring tools and are able to disguise their assaults as normal network activity.

Threat hunting therefore requires a human-focused approach, thinking like an attacker in order to anticipate their actions, before they succeed in infiltrating the network. But most firms aren't taking advantage of this capability yet. The survey asked, **"Does your organisation employ specific proactive threat hunting individuals as part of your security function?"**.

Only 24 per cent answered yes, demonstrating that threat hunting is far from business-as-usual for the majority of enterprises that could benefit.

Fig. 4 : Does your organisation employ specific proactive 'threat hunting' individuals as part of your security function?

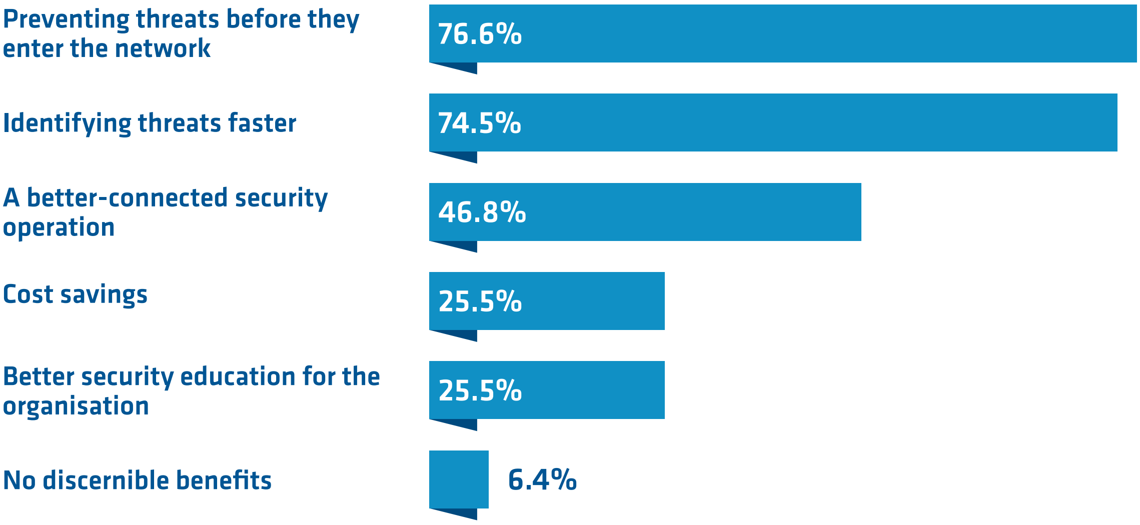


Those that do use threat hunting were asked, **"What benefits has your organisation enjoyed from using threat hunters?"**

The answers included the ability to identify threats faster (75 per cent) and preventing threats before they enter the network (77 per cent). Meanwhile, a quarter of organisations recognise the cost reductions from the possible impact of a breach if it is detected more quickly or prevented entirely as a result of threat hunting.

Clearly, those companies using threat hunting are aware of its benefits.

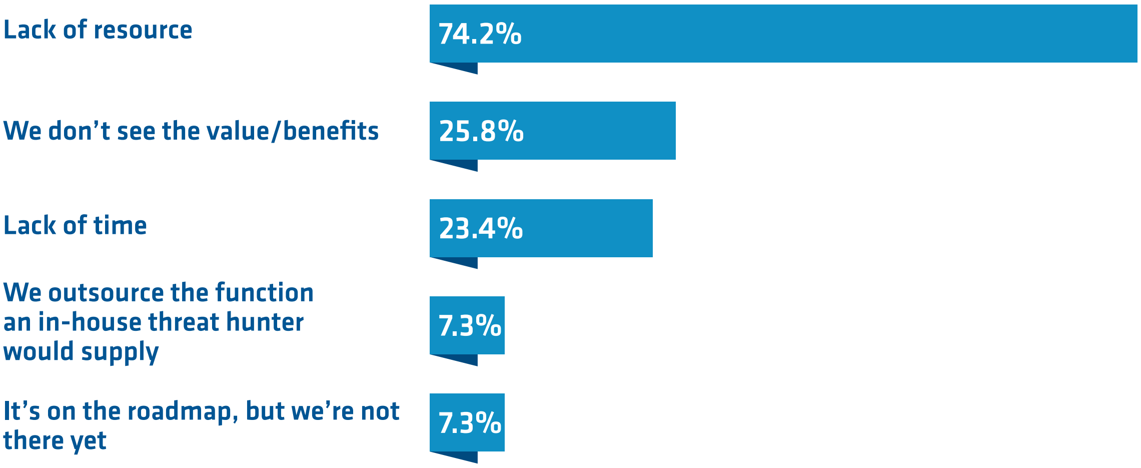
Fig. 5 : What benefits has your organisation enjoyed from using threat hunters? (respondents were asked to tick as many as apply)



But given the reported benefits among those already employing threat hunters, what's stopping more organisations from building threat hunting capabilities into their SOC? When asked this question, the top answer by far was a lack of resource, with 74 per cent saying this is why they don't use this potentially valuable function. However, another quarter (25.8 per cent) said they could not see the benefits. More needs to be done to show organisations how cyber- attacks can be thwarted in this way.

As the survey shows, some firms do not yet use threat hunters but it's on their roadmap: the majority of these (56 per cent) aim to look at employing such talent within the next six months to one year. And two years from now, all those organisations plan to use threat hunters to help fight cyber- attacks.

Fig. 6 : For those who do not currently employ 'threat hunters' – why not? (respondents were asked to tick as many as apply)



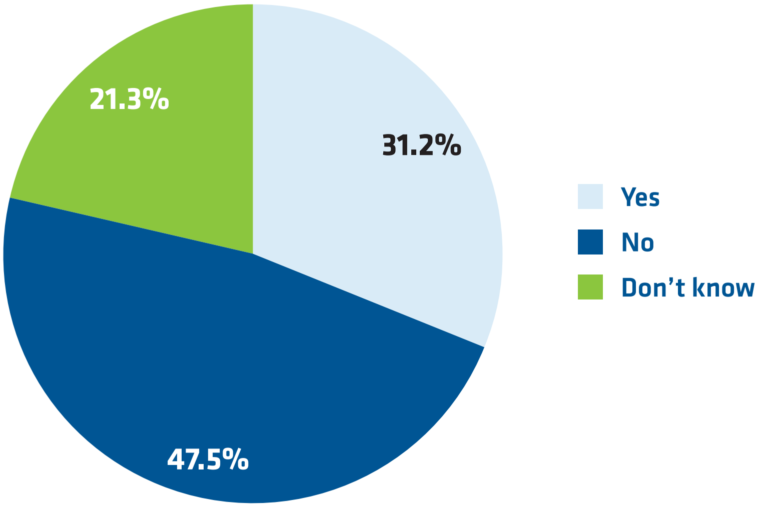
Getting the leadership team on board

It's true that threat hunting offers business benefits, such as increased control and the ability to counter ever-more complex cyber attacks. But leadership buy-in is key to investment in threat hunting. This is partly about positioning ROI in the right way. It's also about budgets.

According to our survey, a third of boards demand provable ROI on security operations. It's certainly a challenge, and it makes proactive protection that much harder.

However, the cost of security breaches is rising. On top of the damage to reputation and operational disruptions, the EU General Data Protection Regulation (GDPR) stipulates that fines of up to four per cent of turnover can be applied to those firms that suffer a breach. This can end up costing tens of millions of pounds. In this environment – with growing security threats on the one hand and risk and compliance considerations on the other – boards are becoming more aware that investment in proactive threat monitoring tools offers potentially significant ROI.

Fig. 7 : Does your board demand provable ROI on your security operations?



Effective threat hunting

Anyone can say they are threat hunting, but firms also need to make sure this activity is performed effectively, and the resulting intelligence is incorporated into the collective consciousness of the SOC to protect the network from similar attacks in future.

Threat Hunters must ensure they have visibility of the whole business, so they have a 'big picture' on what's really happening across the organisation. As part of this, the entire security team should be involved, and a culture of threat hunting instigated across the enterprise.

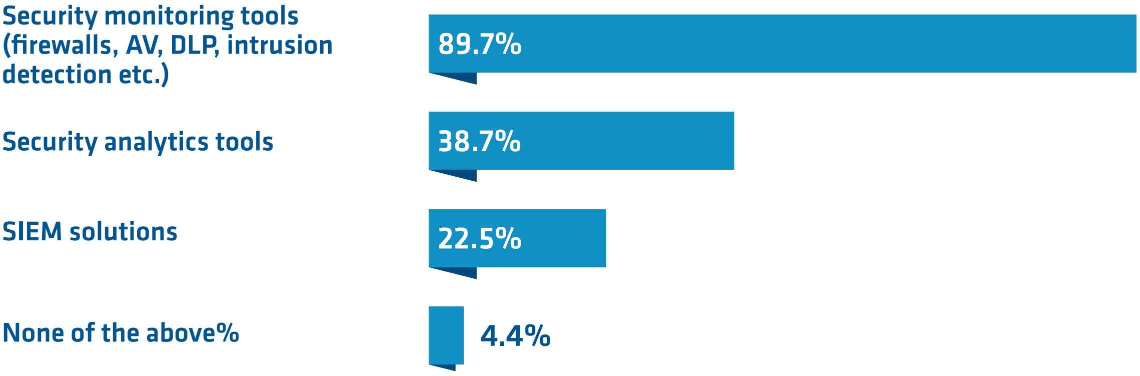
It's important to note that threat hunting is most effective alongside certain security tools. For example, if threat hunters have access to unfiltered data from endpoints, they can complete fast searches, automatically detect suspicious behaviour and correlate network, endpoint and SIEM information. This helps them to pinpoint issues and makes threat hunting more intelligent and effective.

In addition, firms should ensure 24/7 monitoring in real time on every endpoint within the business and must house data centrally, rather than over the network. This allows the true analytic power of unfiltered information to be realised and anomalies flagged for investigation by the threat hunting team.

The survey asked, **"Which of the following types of security tools does your organisation use at an endpoint level?"**. A large number of respondents (90 per cent) said their company uses security monitoring tools such as firewalls, antivirus, data loss prevention and intrusion detection.

Meanwhile over a third (39 per cent) use security analytics tools, while a quarter (23 per cent) take advantage of SIEM solutions. It shows the basic technology is often in place, but it needs to be brought together and the data provided to threat hunters to analyse and act upon.

Fig. 8 : Which of the following types of security tools does your organisation use at an endpoint level? (respondents were asked to tick as many as apply)



Cyber insurance: A worthwhile investment?

Data breaches are increasingly expensive, leading many firms to consider taking out cyber insurance. Cyber insurance has been around since security came to the fore in the 1990s, but the area has never really taken off. However, it could be argued that the concept of such insurance may increase in significance inas potentially huge GDPR fines put a more tangible figure on the cost of a data breach.

That's all well and good, but it can be hard to find an insurance firm that offers a transparent protection model and clarity around the different potential types of breaches. Do cyber iinsurance firms have the right framework and sufficient governance in place to ensure that organisations know just what they are paying for and what the circumstances of a successful claim will be?

Despite these uncertainties, many firms think insurance is a good idea: 31 per cent of those surveyed said they do currently take out cyber security insurance.

Of those that do take out insurance, it isn't a major element of the security budget: Over a third spend less than 20 per cent of their budget on cyber security insurance.

The idea of cyber insurance within today's threat environment is interesting, but multiple questions remain. For example, will cyber insurance actually pay out if a GDPR fine is issued? If so, with bills potentially reaching millions, it will certainly be hard to price insurance post-GDPR.

Fig. 9 : How much of your security budget is spent on cyber security insurance?

1-5 per cent	12.9%
6-10 per cent	11.9%
11–20 per cent	9.9%
21–30 per cent	2.0%
31–40 per cent	1.0%
61–70 per cent	1.0%
41–50 per cent	0.5%
Don't know	41.6%

Conclusion: Threat hunting is rising up the agenda, but awareness of its real potential needs to increase

Threat hunting is starting to rise up the security agenda. As the survey shows, there has been a general shift from reactive to proactive security, but not all businesses understand the benefits that an investment in threat hunting can bring.

Only a quarter of businesses are using threat hunters, despite the potential they offer – such as faster breach identification, breach prevention, cost savings and ROI. Crucially, threat hunters can give control back to organisations at a time of surging cyber attacks across multiple vectors, while shifting the balance of power away from attackers, back to defenders. When a breach does inevitably happen, it means firms are on top of it straight away, limiting damage to reputation and possible GDPR fines.

But it's also clear there is a need for more advanced tools to help threat hunters be effective at their jobs. Part of this is about people inside the organisation: every employee should be on board with a firm's security strategy and threat hunters themselves need to ensure they have visibility across the wider business.

Beyond people, technology is also key in supporting a company's security strategy. Although the survey found some firms do have basic monitoring tools in place, they need to do better – especially given that today's attackers are simply bypassing such solutions and infiltrating networks undetected.

In order for the benefits of threat hunting to be realised, threat hunters must have access to unfiltered data from endpoints, enabling them to complete searches quickly, automatically detect suspicious behaviour and correlate network, endpoint and SIEM data.

Threat hunters can then use this information alongside their experience and judgement to assist them in the continuous battle to gain the advantage over cyber criminals and protect their business from sophisticated attacks.

About the sponsor, Carbon Black

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting, and managed services into a single platform with a single agent, single console, and single dataset, making it easier for organizations to consolidate security stacks and achieve better protection. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) enabling customers to defend against the most advanced threats. More than 4,300 global customers, including 35 of the Fortune 100, trust Carbon Black to keep their organizations safe.

Carbon Black and Cb Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and other jurisdictions.

For more information visit:

Visit: www.carbonblack.com

Carbon Black.